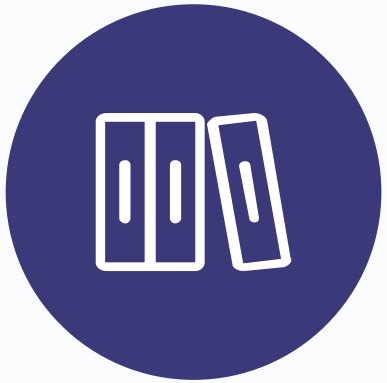
00 课程主要内容

- 第一讲 数据安全概述
- 第二讲 数据分类分级
- 第三讲 数据加密
- 第四讲 数据脱敏
- 第五讲 数据访问控制
- 第六讲 数据水印
- 第七讲 数据容灾备份
- 第八讲 数据安全销毁



第2章 数据分级分类

成都信息工程大学 白杨 alicepub@163.com

2024年10月30日

第2章 数据分级分类

本讲内容概要：

01 第一节—数据元素

02 第二节—数据分类

03 第三节—数据分级

04 第四节—数据分类分级综合案例

第2章 数据分级分类

本讲内容概要：

01 第一节—数据元素

02 第二节—数据分类

03 第三节—数据分级

04 第四节—数据分类分级综合案例

01 2.1 数据元素

数据元素（data element）

通过定义、标识、表示以及允许值等一**系列属性描述的数据单元**。在特定的语意环境中被认定为不可再分的最小的数据单元。一个数据元素一般由**对象类、特性和表示**三部分组成。

对象类

- 现实世界中的想法、抽象概念或事物的集合，表明数据元素所属的事物或概念，在数据元素中占据主导地位。
- **用于收集和存储数据的事物**，例如船舶、教师和发票等。

特性

- 对象类中的所有个体所共有的某种显著的、有区别的性质。
- **用于区别和描述对象，构成对象类的内涵**，例如种类、年龄和价格等。

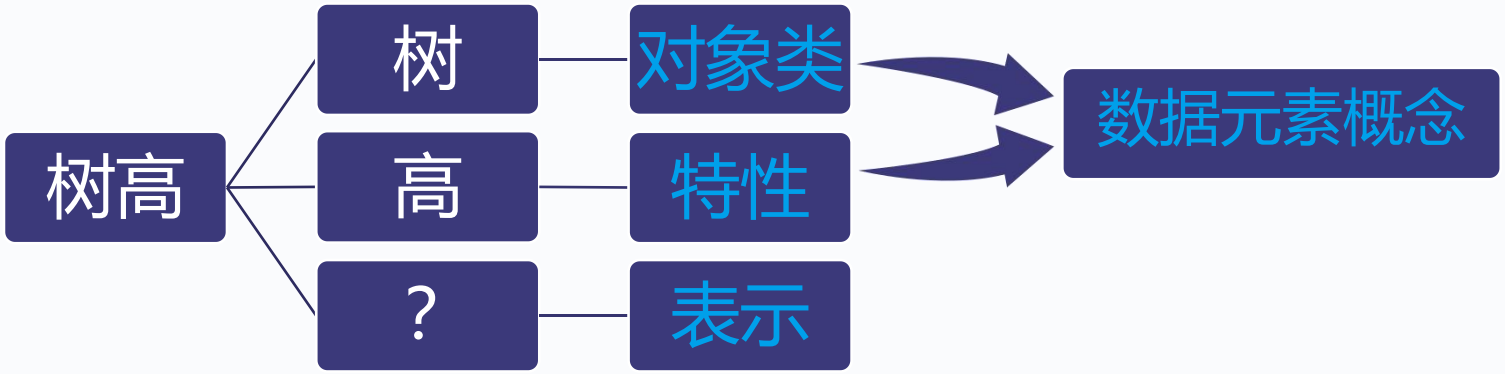
表示

- 值域、数据类型的组合，必要时也包括度量单位或字符集，描述了数据元有效值集合的格式。
- **用于描述数据的形式**，其中最重要的方面是值域。

01 2.1 数据元素

数据元素概念

对象类和特性的组合构成了一个**数据元素概念**。数据元素概念是能够以数据元素的形式表示的概念，不包含具体的表示。



- 树，作为一个对象类，泛指任何一棵树，而非特指某一棵具体的树。
- 将树的高度作为其特性，得到的树高可视为一个对象类加上一个特性（**数据元素概念**），但尚未形成一个数据元素，因为尚未从多种度量树高的方式中选择出一个确定的表示形式。

01 2.1 数据元素

数据元素名称

用于标识数据元素的主要手段，由一个或多个词构成的命名。

语法规则:

- 数据元素名称中，对象类词、特性词和表示词都有且只有一个。
- 对象类词位于名称的第一（最左）位置，特性词位于第二位置，表示词位于最后位置。
- 当表示词与特性词有重复时，可以将冗余词删除。如在描述人的姓氏的数据元素“Person Last Name”中，第二个 “Name” 是数据元素的表示词。为了使表达更清晰，将重复的词删除，即一般使用 “Person Last Name” 来描述该数据元素。
- **唯一性原则**：在同一语境中，所有数据元素名称都是唯一的。

01 2.1 数据元素

数据库系统中的数据元素

- 数据元素出现在数据库或文件中，是一个组织管理数据的基本单元。在组织内部，数据库或文件由记录、段和元组等组成，而记录、段和元组则由数据元素组成。
- **关系型数据库**中的数据元素以字符列的形式出现于表格中。

关系型数据库中与数据元素对应的术语

数据元素		对象类	特性	表示
关系型数据库系统	表	行	列	数据值

数据库表格中的数据元素

记录	雇员			
属性	号码	姓	出生日期	工资额
数据值	1	刘	1970/09/10	8,000
	2	李	1982/01/05	6,000
	3	张	1985/06/20	5,000

- 数据元素允许值的集合称为**值域**。数据元素从不以单一数值的形式表示，因为它代表的是一个类而不是单一实例。
- 例如，雇员号码是一个数据元素，其值域由一个特定企业中允许值的完整列表描述。在这种情况下，数据值仅是雇员号码所有实例的一个列表。数据元素的每个实例只有一个单一数据值，称为“**数据元素实例**”。

第2章 数据分级分类

本讲内容概要：

01 第一节—数据元素

02 第二节—数据分类

03 第三节—数据分级

04 第四节—数据分类分级综合案例

02 2.2 数据分类

三个问题

- 为什么要数据分类分级呢？ （观看视频）
- 数据分类分级有的重要性是什么？
- 怎么来做数据分类分级？ （国标 数据安全技术 数据分类分级规则

02 2.2 数据分类

数据分类是根据数据的属性或特征，将其按一定的原则和方法进行区分和归类，并建立起一定的分类体系和排列顺序的过程。

数据分类的目的

保护敏感数据

识别和标记出敏感数据，从而采取更严格的安全控制和管理措施，以确保敏感数据不被未经授权的访问和使用。

合理分配资源

将安全资源和控制措施针对性地分配到不同的数据类别中，使得对敏感数据和非敏感数据的保护措施更加有效和经济合理。

便于管理审计

帮助组织建立清晰的数据管理策略和安全控制措施，并为数据审计和监管提供依据。

促进共享交换

有助于标准化数据格式和结构，使得数据更容易在不同的系统和组织之间共享和交换。

02 2.2 数据分类

数据分类的基本原则

01

科学性

基于数据的多维特征以及它们之间的逻辑关系，依据数据的本质和内在规律进行科学系统化的分类。

02

实用性

数据分类应当以基础库建设和数据应用等实际需求为出发点，确保每个类别都包含真实有价值的数据，不设立无价值的类别。

03

稳定性

选择最为稳定和最本质的特征指标和属性指标进行数据分类，一旦分类确定生效，应在一定时期内保持相对稳定不变。

04

扩展性

数据分类应保证类目的可扩展性、兼容性，可适应时间变化、政策变化、业务场景变化或基础库建设规划调整导致的类目增减和数据类型变化等情况。

02 2.2 数据分类

数据分类的基本方法

- **线分类法**是一种简单直接的分类方法，其基本思想是将数据根据某种特征或属性分为两个或多个不同的类别，这些类别之间是相互排斥的，不会有重叠。
- 线分类法适用于针对一个类别只选取单一维度进行分类的场景。

02 2.2 数据分类

数据分类的基本方法

线分类法示例

采用线分类法，将证券期货业数据分成四个层级，第一层级表示基本业务条线，第二层级根据“业务管理主体和范围”进一步细分出业务二级子类，第三层级确定各个业务二级子类下的全部数据，表示数据一级子类，第四层级进一步细分出数据二级子类。

证券期货业数据分类示例（部分）

业务条线		数据	
一级子类	二级子类	一级子类	二级子类
交易	交易管理	成交信息	
		委托信息	
		交易日志信息	订单日志
			成交日志
	投资者管理	投资者基本信息	个人投资者基本信息
			机构投资者基本信息
		投资者开户/账户信息	
		投资者鉴别信息	

02 2.2 数据分类

数据分类的基本方法

- **面分类法**是一种将数据按照多个属性或特征进行分类的方法，形成多维分类结构，不同类别之间可能存在重叠或交叉。
- 面分类法是并行化分类方式，同一层级可有多个分类维度，适用于对一个类别同时选取多个分类维度进行分类的场景。

02 2.2 数据分类

数据分类的基本方法

面分类法示例

对企业进行分类可以采取面分类法，分别从组织形式、行业、地区和经济类型四个维度进行归类。

企业分类示例

组织形式	行业	地理区域	经济类型
个人独资 合伙制企业 公司	科技 制造业 金融 新闻传媒 医疗健康 ……	亚洲 美洲 欧洲 非洲 大洋洲	私营 国有 合资 混合所有制 集体所有制 ……

混合分类法示例

混合分类法是一种点面结合的分类方法，以克服单一分类方法的局限性，达到更好的分类效果。

在面分类法的企业分类示例中，“地理区域”这个分类面确定了五个分类类别，可以利用线分类法进一步划分子类。

地理区域分类示例

宏观地理区域	地理亚区	国家或地区
亚洲	东亚	中国
		日本
		蒙古
		……
	南亚	……
	中亚	……
	东南亚	……
	西亚	……
……		

02 2.2 数据分类

数据分类的基本流程

分类准备

- 调研数据现状；
- 确定分类对象；
- 选择分类维度；
- 选择分类方法。

分类实施

- 拟定实施流程；
- 开发脚本工具；
- 记录实施过程；
- 输出分类结果。

结果核查

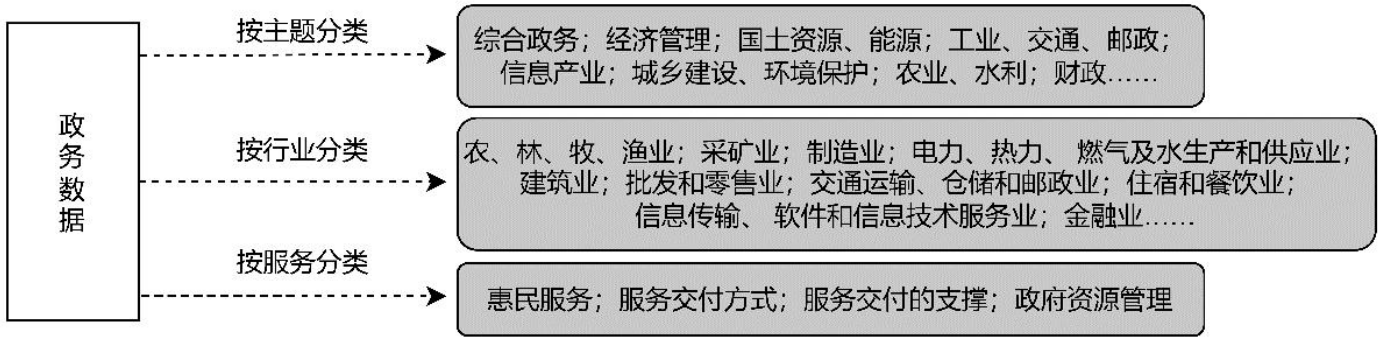
对数据分类表和分类过程记录进行核查，验证分类结果及实施过程是否合规。

02 2.2 数据分类

数据分类案例

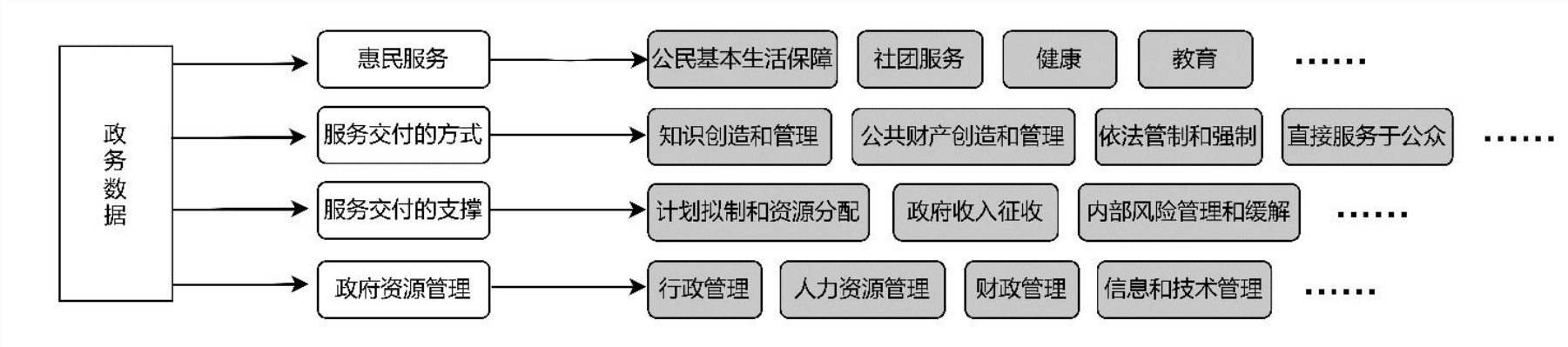
- **分类维度**：主题、行业和服务三个维度。
- **分类方法**：线分类法和面分类结合的混合分类法。
- 在进行政务数据分类实施时，首先采用面分类法，划分为主题分类、行业分类和服务分类三个维度，每个维度按线分类法划分类目。

政务数据——面分类法的结果



- 采用线分类法，在每个维度的一级类目下进一步划分出二级目录。例如，在上述服务分类面中，一级类目可以进一步细分出二级类目。

政务数据——线分类法的结果



第2章 数据分级分类

本讲内容概要：

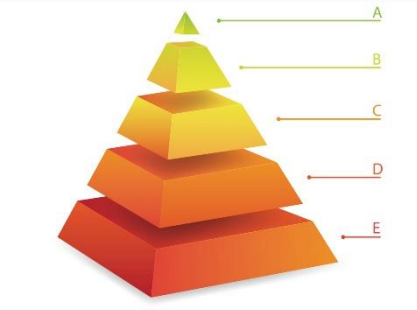
01 第一节—数据元素

02 第二节—数据分类

03 第三节—数据分级

04 第四节—数据分类分级综合案例

02 2.3 数据分级



数据分级是指根据数据的重要程度、数据的敏感程度、数据泄露造成风险程度等，将数据按一定的原则、流程和方法划分为不同等级，并为每个等级制定相应的安全控制和管理策略的过程。

数据分级的目的

优化资源分配

针对不同级别的数据制定相应的安全策略和措施。安全资源可以基于数据的风险等级进行合理分配，避免了资源浪费或分配不当。

引导安全意识

通过公布数据分级政策，可以引导用户理解不同数据的敏感度和重要性，提高用户的数据安全意识。

生命周期管理

数据分级可以指导各级别数据的采集、汇聚、传输、存储、加工、共享、开放、使用、销毁等环节的管理工作。

指导应急响应

在发生数据泄露或其他安全事件时，数据分级信息有助于正确评估风险，采取针对性的应急措施，从而更有效地响应和恢复。

02 2.3 数据分级

数据分级的基本原则

合法合规

遵循相关法律法规及行业主管部门的规定要求，优先对国家或行业有专门管理要求的数据进行定级管理。

自主定级

数据分级应根据本机构自身数据管理需要，在国家数据分级标准的框架下自主确定数据的安全级别。

01 02 03 04 05

分级明确

数据分级的各级别应界限明确，不同级别的数据采取不同的保护措施。

就高从严

当多个因素可能影响数据分级时，按照可能造成的最高影响对象和影响程度确定数据级别。

动态调整

根据数据的业务属性、重要性和可能造成的危害程度的变化，对数据分级、重要数据目录等进行定期审核并及时调整。

02 2.3 数据分级

数据分级的基本方法

数据分级要素			
定性要素	领域 群体 区域 重要性	**定量要素**	精度 规模 覆盖度

数据分级框架

- 根据数据在经济社会发展中的重要程度，以及一旦遭到泄露、篡改、损毁或非法获取、使用、共享后，对国家安全、公共利益或个人、组织合法权益造成的危害程度，将数据从高到低分为**四级、三级、二级和一级**共四个级别。

数据分级要素

- 确定了数据分级的对象后，首先应识别数据分级要素情况。
- 影响数据分级的要素包括定性要素和定量要素，这些要素是用于评估和确定数据安全级别的关键因素。每个要素都从不同的角度反映了数据的特性和潜在风险，它们在数据分级流程中起到了至关重要的作用。

02 2.3 数据分级

数据分级的基本方法

影响对象

- **影响对象**是指数据安全事件可能影响的对象。
- 数据分级需要考虑的影响对象划分为**国家安全、公共利益、组织权益和个人权益。**

影响程度

- **影响程度**是指发生数据安全事件后所产生影响的大小。
- 从高到底划分为**严重损害、一般损害和轻微损害。**

影响程度	定义
轻微损害	数据遭到泄露、篡改、损毁或非法获取、使用、共享后，对影响对象的运行、资产、安全及合法权益造成轻微损害，范围较小、程度可控，结果可以补救。
一般损害	数据遭到泄露、篡改、损毁或非法获取、使用、共享后，对影响对象的运行、资产、安全及合法权益造成较为严重的损害，范围较大、程度可控、结果可以补救或范围较小、结果不可逆但可以采取措施降低损失。
严重损害	数据遭到泄露、篡改、损毁或非法获取、使用、共享后，对影响对象的运行、资产、安全及合法权益造成严重损害，影响的范围、程度不可控且结果不可逆。

数据影响分析

数据影响分析是数据分级过程中的一项关键活动，它涉及评估数据泄露、篡改、损毁、非法获取、使用、共享可能对不同对象造成的影响及其严重程度，是确定数据安全级别的重要判断依据。主要从**影响对象**与**影响程度**这两个方面进行数据影响分析。

02 2.3 数据分级

数据分级的基本方法

数据分级参考规则

在分级要素识别、数据影响分析的基础上，确定数据级别的规则。

影响对象	影响程度			
	严重损害	一般损害	轻微损害	无损害
国家安全	四级数据	四级数据	四级数据	一级数据
公共利益	四级数据	四级数据	三级数据	一级数据
组织权益	四级数据	三级数据	二级数据	一级数据
个人权益	四级数据	三级数据	二级数据	一级数据

数据分级基本规则

- 按照分级参考规则，识别四级数据、三级数据、二级数据和一级数据。
- 当分级要素涉及多个要素、多个影响对象或影响程度时，应按照就高从严原则确定数据级别。
- 数据集级别可基于数据项级别，按照就高从严的原则确定。通常情况下，将数据集中包含的数据项的最高级别作为数据集的默认级别。然而，同时也应考虑到分级要素（例如数据规模）可能会发生变化，需要相应地调整数据集的级别。
- 根据数据重要程度和可能造成的危害程度的变化，应对数据级别进行动态更新。

02 2.3 数据分级

数据分级的基本流程

确定分级对象

确定待分级的数据，如数据项、数据集等。

分级要素识别

结合数据自身的类型、特征和规模，识别数据涉及的分类要素情况。

数据影响分析

结合数据分级要素识别情况，分析数据一旦遭到泄露、篡改、损毁或非法获取、使用、共享后，可能影响的对象和影响程度。

综合确定级别

按照数据分级基本规则，综合确定数据级别。

02 2.3 数据分级

数据分级案例

- **基础电信企业数据**指的是基础电信企业生产经营和管理活动中产生、采集、加工、使用或管理的网络数据或非网络数据，分级对象为最小数据项。
- 根据基础电信企业数据重要程度和敏感程度，确定数据资源的安全等级。

基础电信企业数据分级示例（部分）

数据级别	数据项	内容
四级数据	实体身份证明	身份证、护照、驾照、营业执照等证件影印件；指纹、声纹、虹膜等
	用户私密资料	揭示个人种族、家属信息、居住地址、宗教信仰、个人健康、私人生活等用户私密信息；《征信业管理条例》等法律、行政法规规定禁止公开的用户其他信息
	用户密码及关联信息	用户网络身份密码及关联信息，如：手机客服密码，以及与密码关联的密码保护答案等
	联系人信息	用户通讯录、好友列表、群组列表等用户资料数据
	……	
三级数据	自然人身份标识	客户姓名、证件类型及号码、驾照编号、银行账户、客户实体编号、集团客户编号、集团客户名称等
	用户使用习惯分析数据	用户偏好、消费习惯，通话、短信频次、上网等数量与频次等。
	用户上网行为相关统计分析数据	用户网络行为、用户画像等
	企业发展战略	战略计划、战略风险评估等
	……	

第2章 数据分级分类

本讲内容概要：

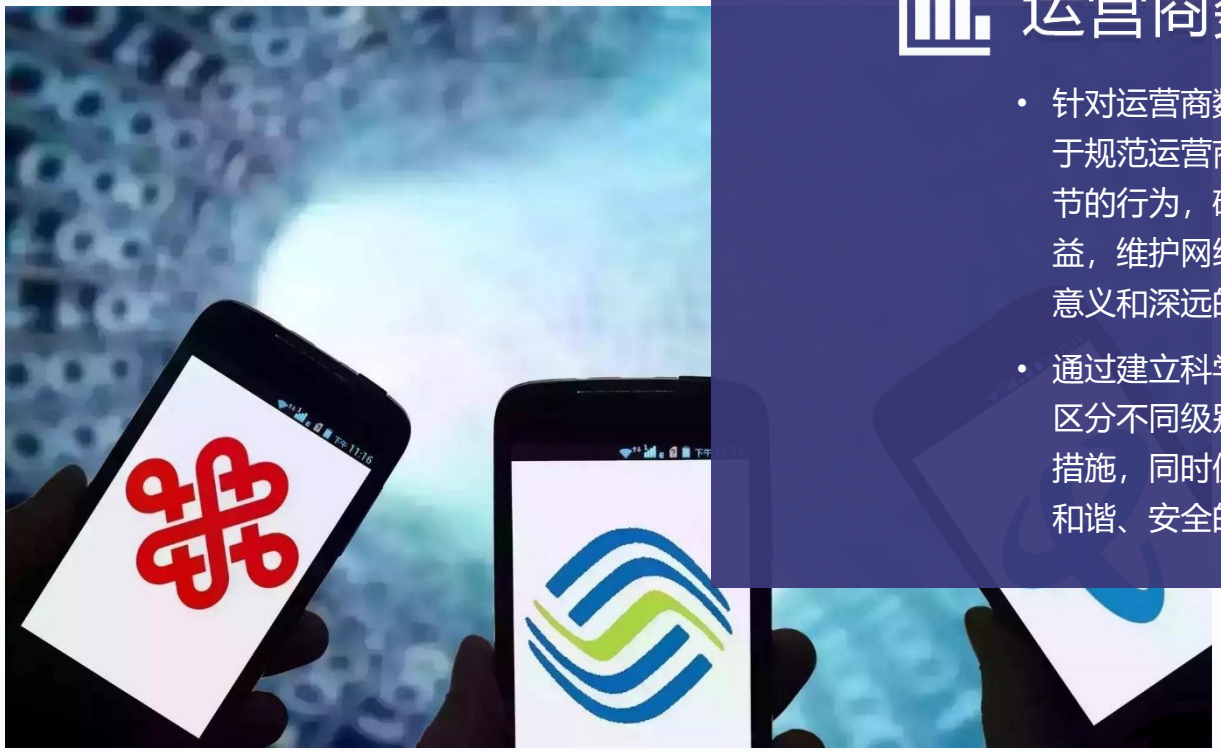
01 第一节—数据元素

02 第二节—数据分类

03 第三节—数据分级

04 第四节—数据分类分级综合案例

02 2.4 数据分类分级综合案例



运营商数据分级分类

- 针对运营商数据面临的安全挑战，进行数据分类分级，对于规范运营商在数据收集、存储、处理、传输、共享等环节的行为，确保数据的合法合规使用，保护用户的隐私权益，维护网络空间安全和社会公共利益，具有重要的现实意义和深远的战略价值。
- 通过建立科学合理的数据分类分级体系，可以有效识别和区分不同级别的数据，对高风险数据采取更加严格的保护措施，同时促进数据资源的合理利用和安全流通，为构建和谐、安全的网络环境提供有力支撑。

02 2.4 数据分类分级综合案例

数据分类

运营商数据分类方法采用线分类法分为两层，第一层由13个一级子类组成，第二层由一级子类的数据元素组成。

分类对象

- 运营商在提供通信服务过程中收集和生成的，能够反映用户通信行为、位置轨迹、消费习惯等各类信息的数据集合。

分类维度

- 按照业务属性（或特征），对运营商数据进行一级子类的划分；
- 按照一级子类内部的数据隶属逻辑关系，将每个一级子类的数据进一步细分为若干个二级子类。

分类类别

- 运营商数据被分为13个一级子类，第二层细分成相关的数据元素；
- 例如，一级子类“**消费信息**”下包括预存款、缴费情况、付费方式、话费余额、受赠情况、交易历史记录等数据元素。

02 2.4 数据分类分级综合案例

数据分级

针对运营商数据发生泄露、篡改、损毁或非法获取、使用、共享后的影响对象、影响程度等要素，进行了数据分级，包括一级、二级和三级3种数据级别。

确定分级对象

01

在该运营商数据分级示例中，结合运营商数据量具有较大范围影响规模的背景，单纯针对单个数据项进行分级判定。

分级要素识别

02

以二级子类“**通话详单**”为例，需要识别的要素包括数据的精度（如通话记录的详细程度）、规模（涉及的用户数量）、覆盖度（数据覆盖的地理范围）等。

数据影响分析

03

如果通话详单数据泄露，可能对用户的隐私权造成损害，影响程度可能从轻微到严重不等，具体取决于泄露数据的规模和类型。同时，数据泄露还可能对运营商的声誉和客户信任造成损害。

综合考虑大多数情况下通话详单的数据类型、规模和一旦泄露所造成的实际损害程度等，可以认为通话详单数据遭受安全威胁时，直接**对个人利益产生一般损害**。

综合确认级别

04

基于分级要素识别和影响分析的结果，将通话详单数据判定为**三级数据**。

02 2.4 数据分类分级综合案例

分类分级结果

运营商数据分类分级参考结果

数据类目（一级子类）	数据元素（二级子类）	影响对象	影响程度	数据级别
位置数据	装机地址	自然人	一般损害	三级
	行踪轨迹	自然人	一般损害	三级
	位置经纬度	自然人	一般损害	三级
	小区代码	自然人	一般损害	三级
	基站编号	自然人	一般损害	三级
	位置文字描述	自然人	一般损害	三级
通信详单	通话详单	自然人	一般损害	三级
	短信详单	自然人	一般损害	三级
	彩信详单	自然人	一般损害	三级
	增值业务详单	自然人	一般损害	三级
	上网流量详单	自然人	轻微损害	二级
部分用户画像	交往圈	自然人	轻微损害	二级
	家庭信息	自然人	轻微损害	二级
用户业务基本信息	用户状态	自然人	轻微损害	二级
	入网方式	自然人	轻微损害	二级
	入网起止时间	自然人	轻微损害	二级
	在网时长	自然人	轻微损害	二级
	停开机	自然人	轻微损害	二级
	协议起止时间	自然人	轻微损害	二级
	消费额度	自然人	轻微损害	二级
	发展渠道	自然人	轻微损害	二级
	发展人	自然人	轻微损害	二级
业务订购信息	业务订购	自然人	轻微损害	二级
合同信息	集团客户业务合同	其他机构	轻微损害	二级
	个人客户协议	自然人	轻微损害	二级
	优惠信息	自然人	轻微损害	二级
围栏信息	是否在规定围栏范围内	自然人	一般损害	三级
消费信息	预存款	自然人	一般损害	三级
	缴费情况	自然人	一般损害	三级
	付费方式	自然人	一般损害	三级
	话费余额	自然人	一般损害	三级
	受赠情况	自然人	一般损害	三级
	交易历史记录	自然人	一般损害	三级
账单	固定费用	自然人	一般损害	三级
	通信费用	自然人	一般损害	三级
	欠费信息	自然人	一般损害	三级
客户服务信息	服务等级	自然人	轻微损害	二级
	信用等级	自然人	轻微损害	二级
	信用额度	自然人	轻微损害	二级
	积分	自然人	轻微损害	二级
	VIP 信息	自然人	轻微损害	二级
服务日志	Cookie 内容	自然人	轻微损害	二级
	上网日志	自然人	轻微损害	二级
	APP 使用日志	自然人	轻微损害	二级
	软件使用记录	自然人	轻微损害	二级
	点击记录	自然人	轻微损害	二级
部分用户画像	兴趣爱好	自然人	轻微损害	二级
	APP 偏好	自然人	轻微损害	二级
	终端偏好	自然人	轻微损害	二级
	内容偏好	自然人	轻微损害	二级
违规记录	垃圾短信记录	自然人	无损害	一级
	骚扰电话记录	自然人	无损害	一级
	诈骗电话记录	自然人	无损害	一级
	黑名单	自然人	无损害	一级

谢谢！